China's Cybersecurity landscape from the perspective of CNCERT/CC

OUTLINE

The cybersecurity landscape of mainland China

Introduction about CNCERT and responses to cybersecurity threats

Network development

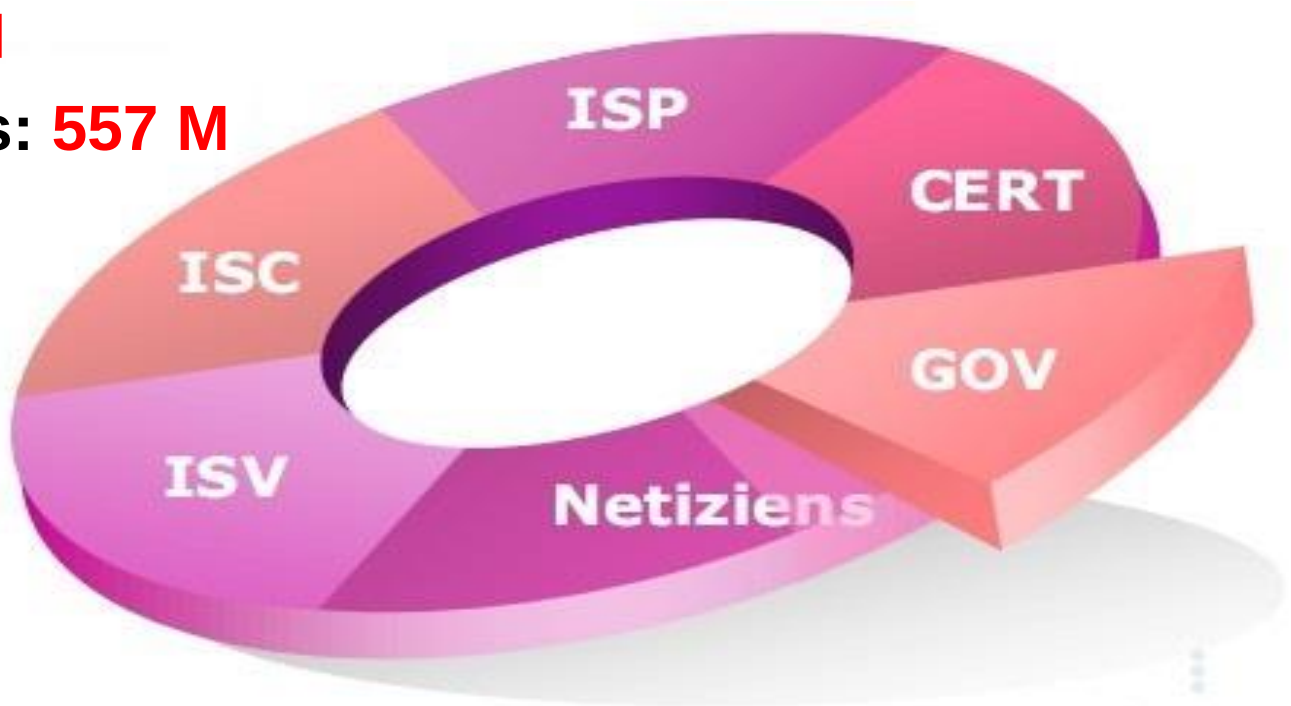
Statistics (until 2014):

Domain name : 21M

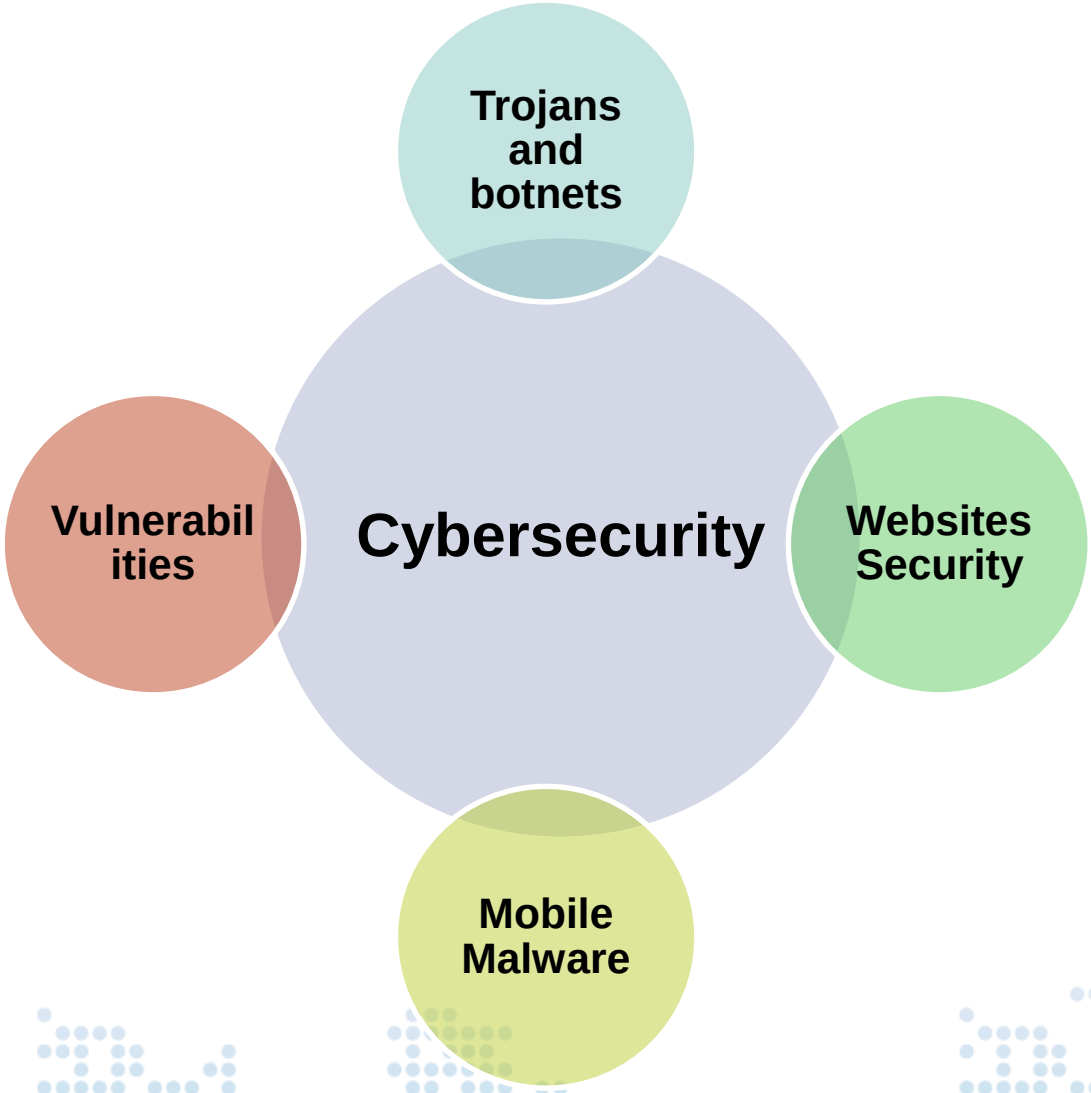
Website :34 M

netizens: 649 M

mobile netizens: 557 M

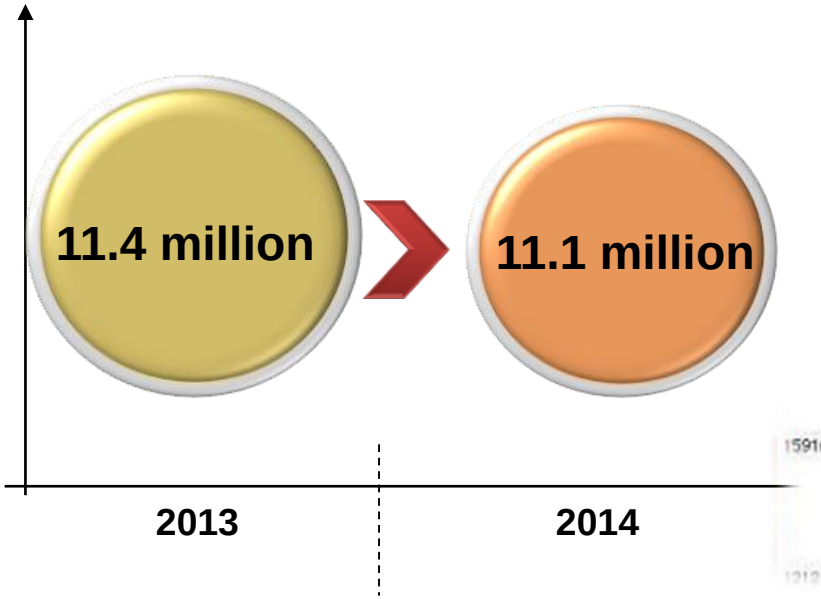


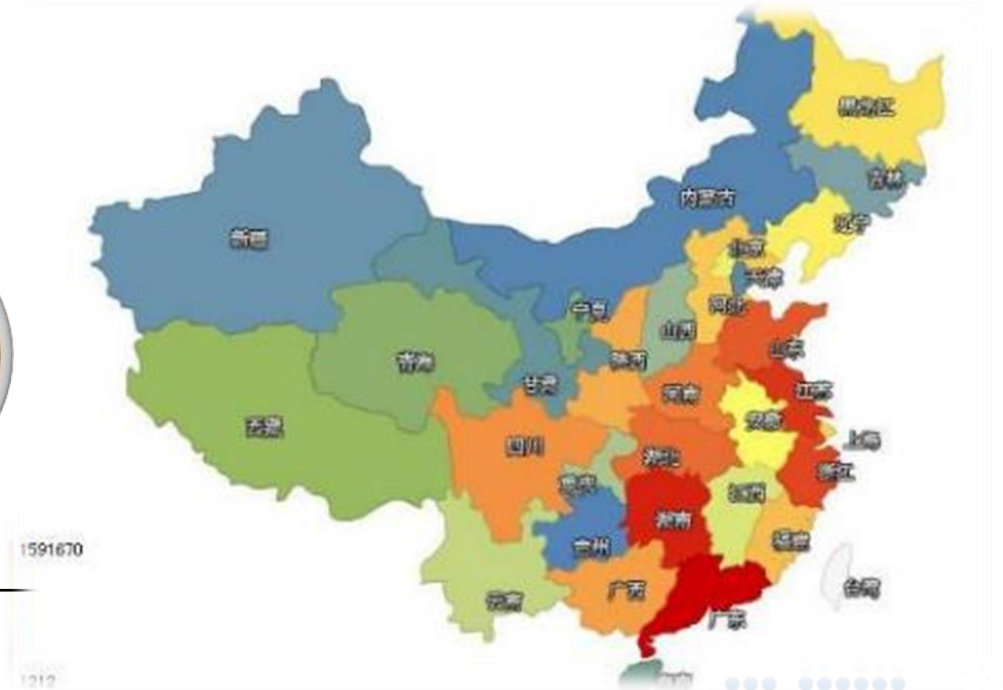
Cybersecurity landscape



Trojans and botnets

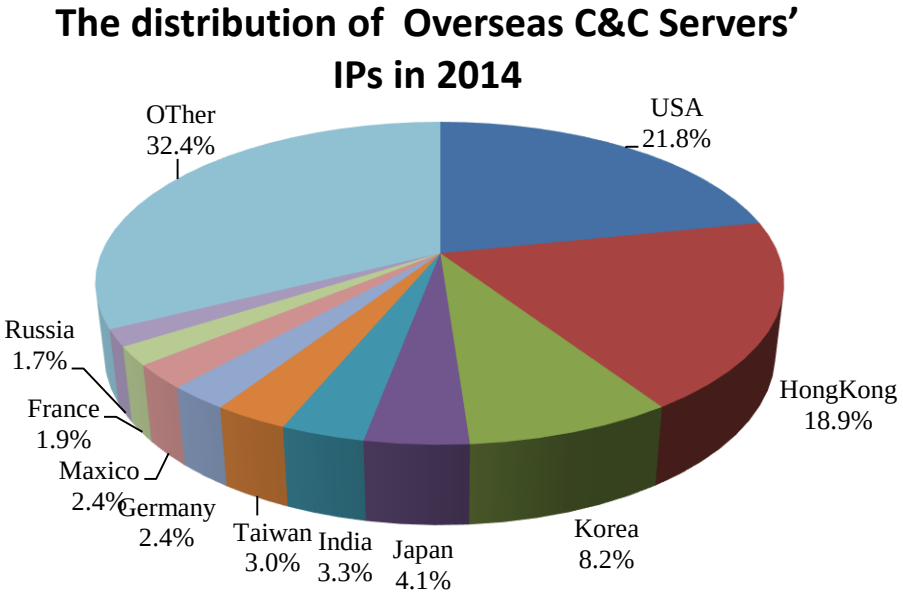
In 2014, a total of over 11.1 million computers were infected with trojans or botnets in mainland China, about 2.3% less than 2013.





Massive infected computers were controlled by overseas C&C servers

More than 10.8 million infected hosts were controlled by about 42 thousands trojan or botnet C&C servers located overseas.



- The top 3 locations of the C&C server's IPs were the USA (21.8%), Hongkong(18.9%) and Korea(8.2%).
- The C&C servers in the USA controlled more than 3.9 million infected hosts in mainland China, which recorded the largest amount. It was followed by Portugal and Finland.

Website security

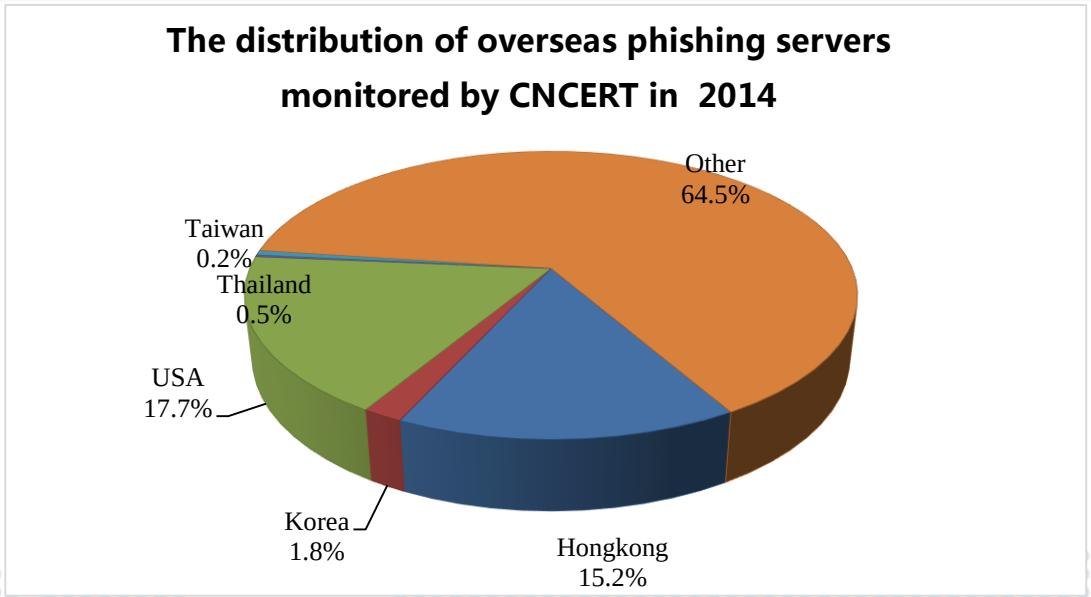
➢Websites defaced : 37 thousand 1.8 thousand government websites ➢Websites planted with backdoors: 40 thousand 1.5thousand government websites	➢Over 19 thousand overseas IPs conducted remote control on over 33 thousand websites in mainland China. ➢In terms of their IP locations: USA (24.8%) Korea(6.7%) Hongkong(6.5%)

Large amounts of phishing pages were located overseas

99 thousand phishing webpages targeted websites in mainland China.

- About 7 thousand IPs were involved.
- 89.4% IPs of these phishing servers were located overseas.
- 1083 IPs from USA loaded more than 10 thousand phishing pages.

CNCERT received about 18 thousand reports of phishing, 31.8% of the total reports.

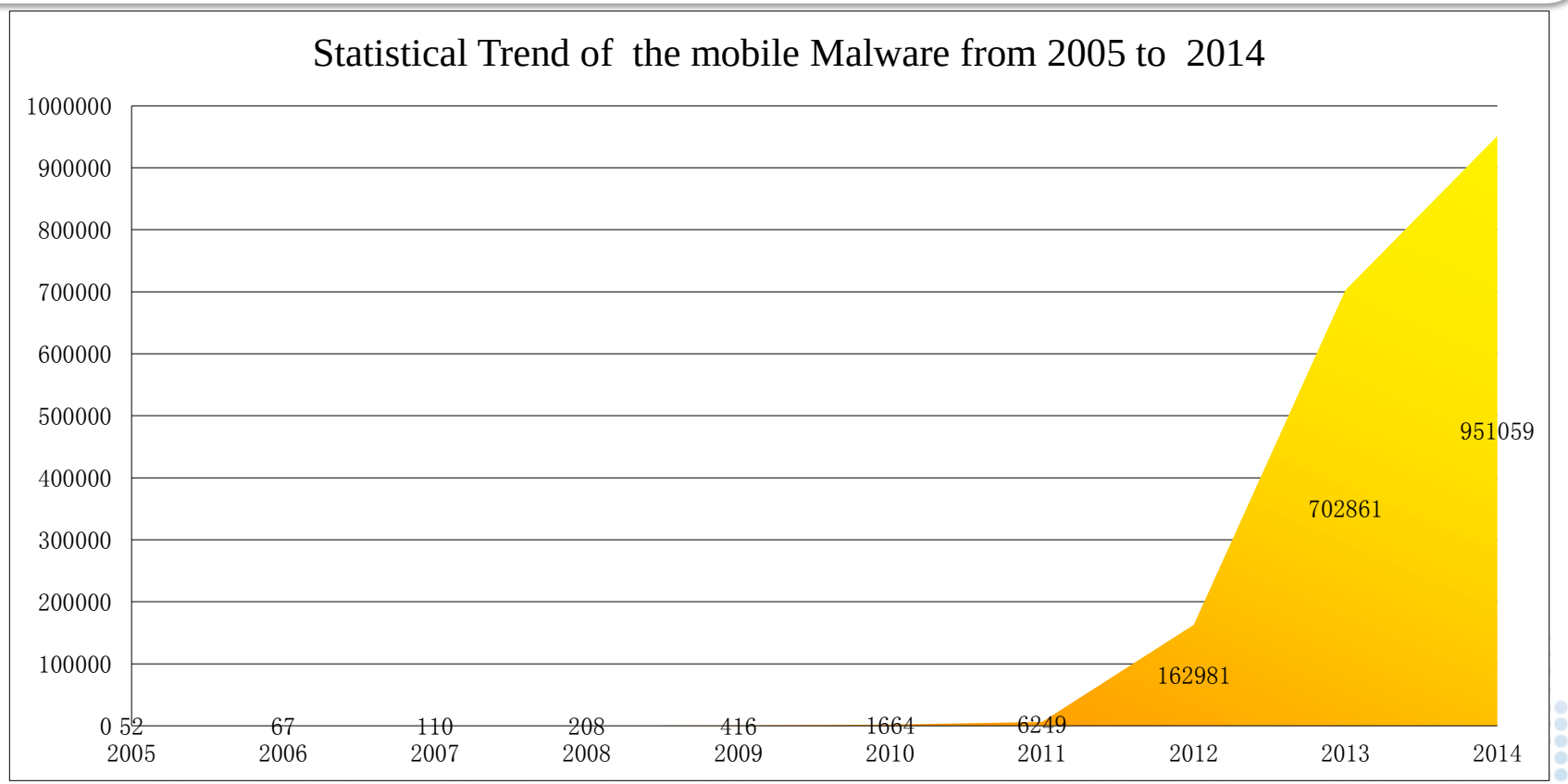


Mobile malware

Over 300 third party android app stores.

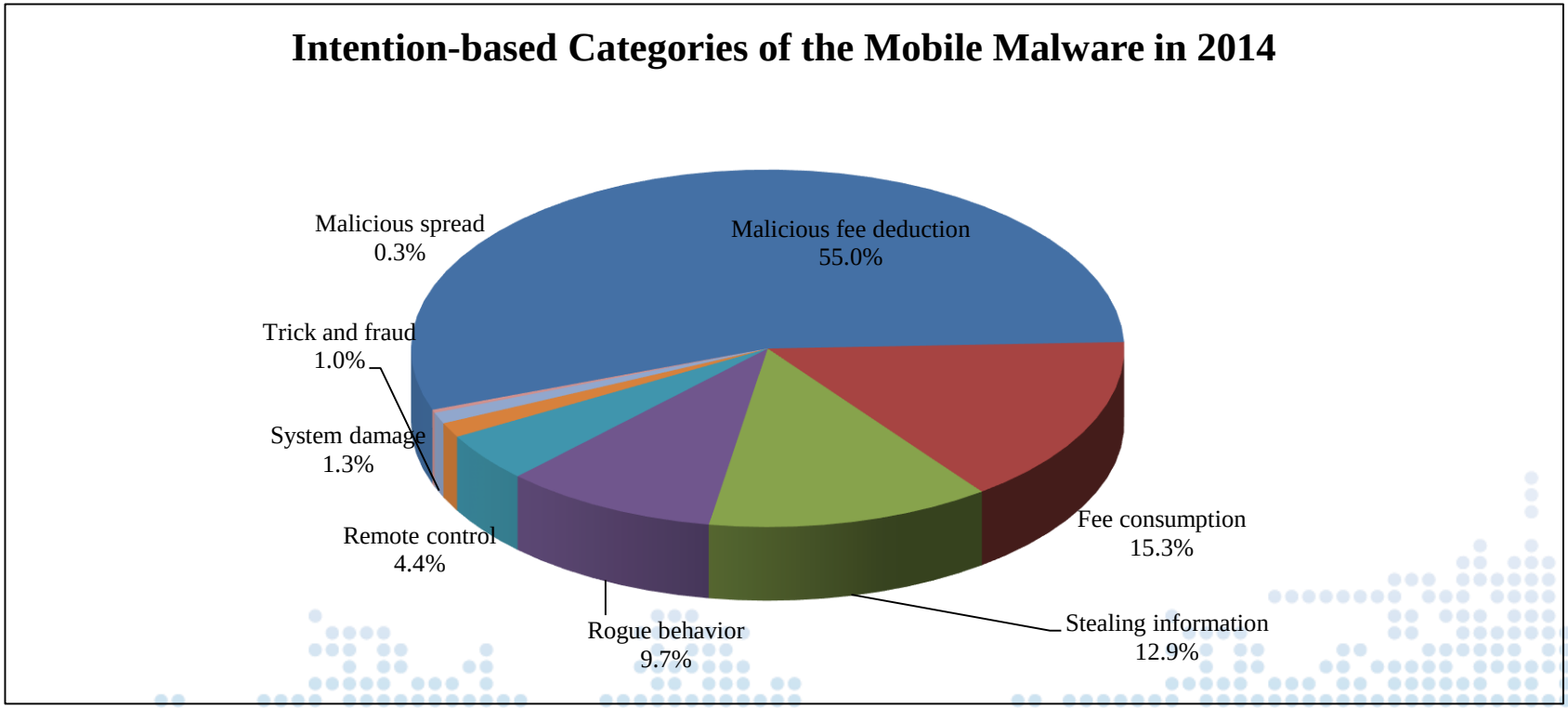
Mobile malware rose rapidly

In 2014, CNCERT captured more than 951 thousand mobile malwares. We found in the last several years, the mobile malware becomes time of growth.



More and more hacker make mobile malware for pursuing interest.

In term of intension of the mobile malware:
- Malicious fee deducting (55.0%)
- fee consumption (15.3%)
- stealing information (12.9%)



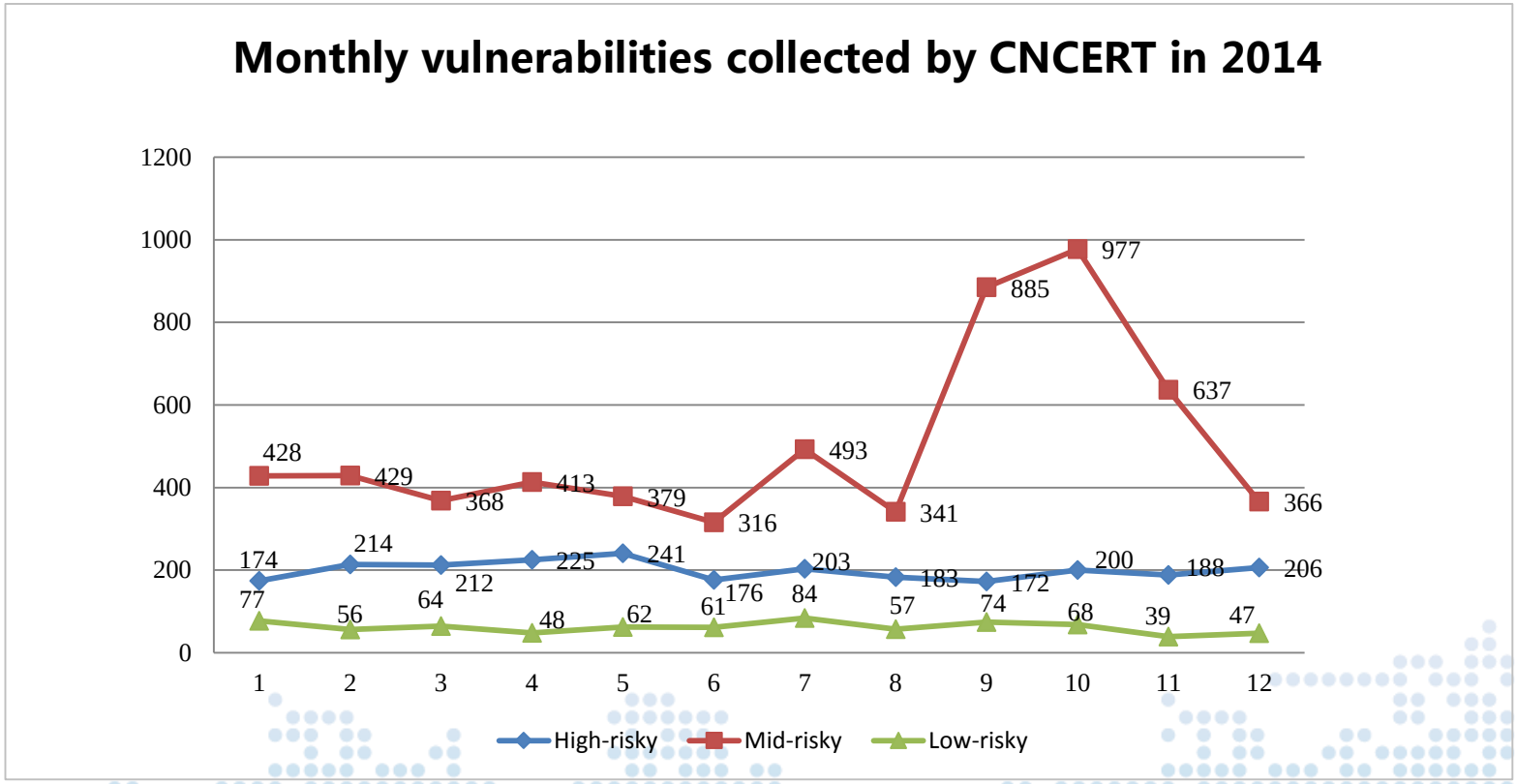
Vulnerabilities

- **Vulnerabilities In total**

9163 ↑ 16.7%

- **High-risky**

2394 ↓ 8.1%



The process of fixing vulnerabilities is too slow to avoid risk

Network administrators are too busy to handle a lot of new vulnerabilities.

It should be very careful to operate on the online systems.

It takes a long time to fix vulnerabilities.

Both accumulated and newly occurred vulnerabilities cause serious threat to information systems.

OUTLINE

The cybersecurity landscape of mainland China

Introduction about CNCERT and responses to cybersecurity threats

National Level CERT of China

2002.9

- **Non-governmental and non-profit cybersecurity technical center under MIIT (Ministry of Industry and Information Technology of the People's Republic of China)**
- **Single point of contact in mainland China for national CERTs**
- **Key coordination team for China's cybersecurity emergency response community**

EARLY WARNING

Received(2014):

800+ information report partners domestic

Released(2014):

264 reports

52 weekly reports in English

1 annual report in English

Landscape presentation

Annual meeting

Content of report include: cybersecurity threats notification, incidents analysis, national landscape analysis, technical assistance ,etc.

Emergency Response

Accepted 56180 incidents complaint

Handled 56072 incidents

Taken down 744 large scale Botnets

protect 982,000 infected hosts

removed 8644 malicious apps

=

Increase the governance intensity of the Internet environment and restrain malicious codes

CNCERT International Cooperation Partnership

CNCERT has established partnership with

144 organizations in 63 countries or regions

Many Thanks!

http://www.cncert.org.cn
Email: cncert@cert.org.cn
ME: Yunqian Zhu
zyq@cert.org.cn